

ABSTRACT OF THE DISCLOSURE

Distributors can verify a signature without acquisition of a certificate for each signer from the certificate authority. A signature part calculates a hash value of distribution information and sets it to a variable h (step S412). Signer private information is taken out from a first signer private information storage part and set to the variable d (step S413). A signature key information selection part takes out signature key information corresponding to a product identifier pid from a signature key information storage part and sets it to the variable t, n (step S414). A signature part calculates a first signature value to the variable h by use of signer private information d and sets it to the variable r1 (step S415). A distribution information generating part calculates a second signature value to the variable h by use of a signature key information t according to the variable h (step S416). A signature value to the final variable h is calculated by use of the results r1 and r2.

55.03.7 534350